The Secure Brief

RSI NEWSLETTER

ISSUE #2607 | DATE: July 2026

CMMC Phase II Suspended

What the Pause Means for the Defense Industrial Base

In a move that resets the compliance calendar for every defense contractor, the Department of Defense has suspended the CMMC Phase II requirements scheduled to take effect November 10, 2026. The pause is effective immediately and halts the transition to third-party certification across Department solicitations and contracts.

The stated reason is cost and access. Officials cited data, including SBA reporting, indicating CMMC compliance was pushing innovative companies out of the Defense Industrial Base and delaying capabilities to the warfighter. A new CMMC Reform Task Force will run a top-to-bottom review and deliver its findings within 60 days.

What is not changing — and this is the part that matters most. The suspension does not eliminate the requirement to protect federal data. Three obligations remain firmly in place:

- Phase I self-assessment requirements stay in effect.
- NIST SP 800-171 Rev 2 remains the enforced standard, through self-assessments and select government-led assessments.
- DFARS clause 252.204-7012 still obligates all contractors and subcontractors to safeguard covered defense information.

The RSI Security read. A suspension is not a reprieve. The organizations that treat this as permission to stop are the ones most exposed when the Task Force reports back and a revised model emerges. Use the pause: shore up your NIST 800-171 self-assessment, close the gaps a certification assessment would have surfaced anyway, and keep your evidence organized so you're ready to move the moment the path forward is clear. Cyber hygiene was always the point.

Based on the Department's official release.

Microsoft's Record Patch Tuesday

Microsoft's June 2026 Patch Tuesday was its largest ever, fixing roughly 200 vulnerabilities — nearly 40 rated critical, spanning Windows, Azure, Office, Outlook, Exchange, and AI tools. The record volume follows Microsoft's reported success using AI to find flaws in its own code, a reminder that AI is accelerating discovery on both sides.

None were exploited in the wild at release, but three were publicly disclosed beforehand and all three carry an "exploitation more likely" rating: a Windows denial-of-service flaw tied to the HTTP/2 "Bomb" technique that can knock web servers offline in seconds (CVE-2026-49160), a BitLocker bypass allowing an attacker with physical access to reach encrypted data (CVE-2026-50507), and a privilege-escalation bug that can elevate to System (CVE-2026-45586). Microsoft also published advisories for 360 third-party component issues, and Adobe patched more than 120 flaws the same day.

What Will be Inside Of The Newsletter

THREAT LANDSCAPE

What Defined July 2026

AI finding twice as many cyber flaws

AI-driven security tools are finding software vulnerabilities twice as fast in 2026 as in 2025 — 45,207 flaws logged already this year, nearly matching all of 2025. Oracle, Microsoft, and Google all hit record highs in July, mostly self-discovered. Exploited-vulnerability counts haven't risen, but attackers who do strike are now 3x faster (24 hours vs. 72 in 2025).

Cyber Actors Exploit Programmable Logic Controllers Across US

CISA, FBI, and NSA warn that Iranian-affiliated APT actors (linked to the CyberAv3ngers/IRGC group) are actively exploiting internet-exposed PLCs from Rockwell Automation, Schneider Electric, and Siemens across US Government Services, Water/Wastewater, and Energy sectors. Actors exfiltrate and tamper with project files, disabling safety shutdown logic and manipulating HMI/SCADA displays — causing operational disruption and financial loss at some victims. Core mitigation: get PLCs off the public internet, enforce MFA/secure gateways for remote access, and check for unauthorized logic changes using vendor integrity tools.

Apple v. OpenAI: A Trade-Secret Case Study in Insider Risk

On July 10, Apple filed suit against OpenAI, alleging the AI company poached Apple employees and coaxed them into handing over confidential material to jumpstart its own hardware business. OpenAI says it is reviewing the filing and has "no interest in other companies' trade secrets."

Set aside the two brand names, and the allegations read like a textbook insider-threat scenario — the kind that plays out far more often than it makes headlines. According to the complaint, departing employees allegedly took confidential files with them, one used an authentication bug to breach the internal network and download dozens of hardware-related documents, and candidates were reportedly asked to bring "actual parts" from their current employer to interviews. Whether the claims hold up in court, the pattern is one every organization should recognize.

Why it matters to you. The most valuable data an organization holds often walks out the door with the people who leave. The 2026 Verizon DBIR put the human element in 62% of breaches, and insider-driven data loss — including employees moving information to personal accounts and devices — remains one of the hardest categories to detect, because the access is legitimate right up until it isn't.

The controls that address it:

- Offboarding discipline. Revoke access immediately on departure, and audit what a leaving employee touched in their final weeks — not just whether their badge still works.
- Data-loss prevention on endpoints. Company laptops leaving with confidential files is a DLP failure. Controls that flag or block large transfers to personal devices and accounts close that gap.

The RSI Security read. Insider risk is not solved with a single tool. It sits at the intersection of access governance, monitoring, and offboarding process — exactly the continuous-posture disciplines that erode between annual reviews. A case this visible is a useful prompt to ask a simple question: if a key employee left tomorrow, would you know what they took?

Source: Based on reporting from The Guardian, July 10, 2026. Allegations are unproven and the litigation is ongoing.

ACROSS THE CYBER REALM

Microsoft's Signals Worth Tracking

01

Tycoon2FA Disruption Impact

Microsoft's March 2026 takedown of the Tycoon2FA phishing-as-a-service platform continued paying off through Q2. Phishing volume linked to Tycoon2FA fell 92% from pre-disruption levels — dropping to 1.5 million messages in May and 1.2 million in June, down from a 15.1 million/month baseline in late 2025. No replacement service emerged at comparable scale, and Tycoon2FA's share of CAPTCHA-gated phishing fell from 76% (Dec 2025 peak) to just 12% by June. After losing Cloudflare protection, the platform shifted over 40% of its new domains to .RU hosting — signaling ongoing rebuilding efforts, but no real recovery.

02

QR Code Phishing Trends

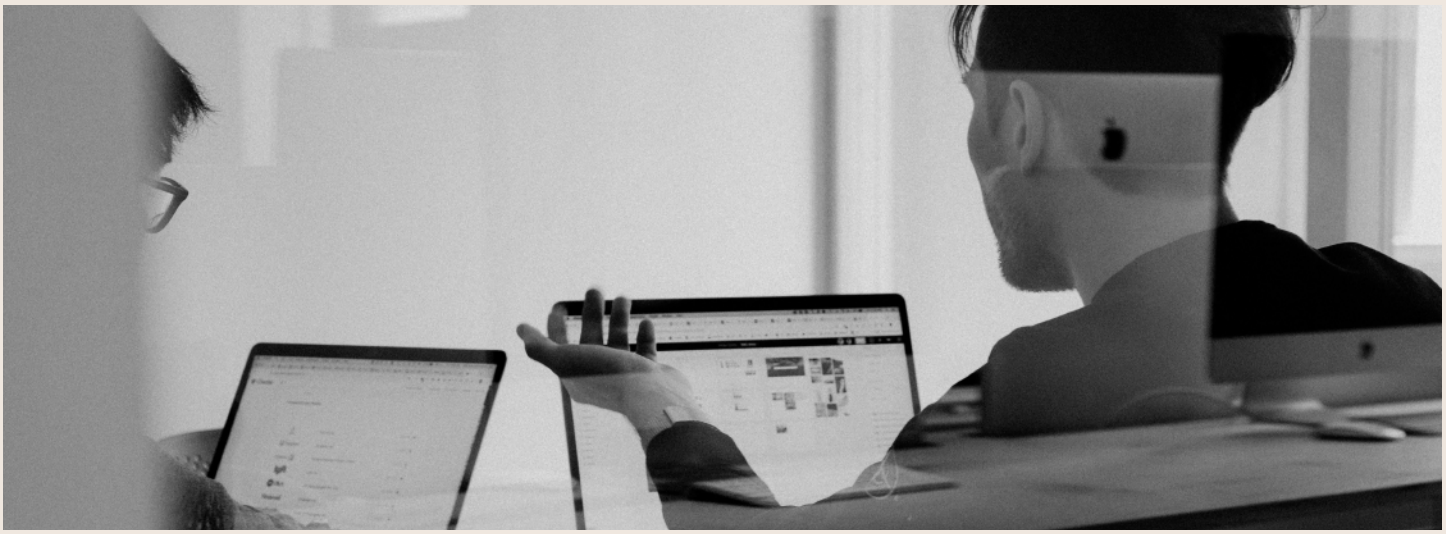
QR code phishing peaked in March at 18.7 million attacks — the highest in over a year — before declining three straight months to 8.3 million by June, back to mid-2025 levels. Delivery methods shifted: PDF attachments (once 79% of QR attacks in April) fell to 58% by June, while DOC/DOCX payloads rose from roughly 20% to 40% over the same period — a rotation pattern Microsoft has seen recur throughout the year. Email-embedded QR codes, which spiked in March, effectively disappeared in Q2.

CAPTCHA-gated phishing volume collapsed 81% from its March peak of ~12 million attacks down to 2.2 million by June — its lowest point in over a year. Payload rotation was rapid and erratic: PDF attachments surged to 63% of attacks in April, then dropped to 22% by June; SVG files fell to a low of 5% in April before climbing back to 26% in June; email-embedded URLs reclaimed the top spot in June (30%) mostly because every other method declined faster, not because URL-based delivery actually grew.

Critical Infrastructure

Microsoft's core recommendations: enable Zero-hour auto purge (ZAP) for retroactive threat response, turn on Safe Links/Safe Attachments, enable network protection in Defender for Endpoint, and move to passwordless authentication (Windows Hello, FIDO keys, Authenticator) wherever supported. For accounts still on passwords, enforce phishing-resistant MFA via conditional access, especially for privileged accounts. Attack simulation training (including Teams-based phishing simulations) and automatic attack disruption in Defender XDR round out the baseline defense stack.

Source: Microsoft Threat Intelligence, "Email Threat Landscape: Q2 2026 Trends and Insights," Microsoft Security Blog, July 23, 2026.



Your Compliance Partner

RSI Security is a trusted leader in cybersecurity and compliance, helping organizations of all sizes strengthen defenses, meet regulatory requirements, and maintain resilience in an evolving threat landscape.

The world's first international management system standard for Artificial Intelligence Management Systems (AIMS). RSI Security provides ISO 42001 readiness and advisory services, preparing organizations for certification by an accredited third-party auditor.

Our multidisciplinary team combines deep expertise in threat detection, vulnerability management, regulatory compliance, and incident response to provide complete protection that grows with your business.

From assessment to automation, RSI Security simplifies cybersecurity, empowering your team to focus on what matters most: innovation, growth, and customer trust.

SERVICE HIGHLIGHT

Security That Does Not End at the Assessment

ISO 42001 Readiness Advisory

As organizations adopt AI faster than they can govern it, ISO/IEC 42001 has emerged as the benchmark for demonstrating that AI is managed responsibly. Published jointly by ISO and IEC, it is the first international standard dedicated to AI management systems, and RSI Security helps organizations get ready for it.

Any organization building, deploying, or relying on AI systems, and facing pressure to demonstrate accountability. While ISO 42001 is not yet a legal requirement, it is quickly becoming a recognized signal of trust across industries. Early alignment reduces uncertainty, prevents fragmented governance, and positions organizations ahead of tightening AI regulatory expectations, the same "prepare now" logic that separates leaders from laggards on every emerging framework.

RSI Security provides ISO 42001 readiness and advisory services. We help organizations define AIMS scope, interpret requirements, integrate AI governance into existing management systems, and build defensible, audit-ready evidence, so that when you engage an accredited certification body, you are prepared rather than scrambling. Certification itself is conducted by an accredited third-party auditor; our role is to get you ready for that process and to keep your governance program strong afterward.

1

AI Risk Visibility

A structured inventory of where AI operates across the business, so shadow AI and ungoverned tools surface before they become liabilities.

2

Regulatory Readiness

A framework aligned to international expectations, positioning the organization ahead of tightening AI regulation instead of reacting to it.

3

Governance & Accountability

Defined ownership, policies, and decision rights across the AI lifecycle, so responsibility for AI outcomes is clear rather than assumed.

4

Stakeholder Trust

Demonstrable proof to customers, partners, and investors that AI is governed responsibly, increasingly a condition of doing business, not a differentiator.

AUGUST 2026

Where the Industry Gathers

AUG 1-6 **Black Hat USA 2026**
Mandalay Bay in Las Vegas, NV
Features expert-led technical trainings (August 1–4), summit day, briefings, and the busin ess hall.

AUG 6-9 **DEF CON 34**
Las Vegas, NV
The iconic annual hacker convention featuring large-scale villages, contests, and talks.

AUG 12-14 **USENIX Security Symposium**
Philadelphia, PA
Bringing together researchers, practitioners, and system administrators to discuss the latest advances in security and privacy.

AUG 19-28 **SANS Security Awareness & Culture Summit 2026**
Caesars Palace & Virtual in Las Vegas, NV
Focuses on building security culture, user awareness, and behavioral change.

> *RSI Security's managed services provide a way to spread the workload out, making sure the actual compliance audit gets done quicker and with lower costs. They worked with us to make sure all the follow-up audits were dealt with."*
>
> **Guido Solares**
> Director of Information Security
> Tilly's

REGULATORY SPOTLIGHT

SEC Chairman's Statement on 2026 Regulatory Agenda

On July 7, 2026, SEC Chairman Paul S. Atkins released a statement on the Commission's 2026 Regulatory Agenda, marking just over one year into his tenure as chairman. Atkins framed the agenda around three core priorities:

- **Crypto policy** — Positioning the U.S. as the "crypto capital of the world" (a stated Trump administration goal) by bringing more crypto products onshore, establishing clearer rules for capital raising with crypto assets, and providing regulatory clarity on how market participants can custody and trade tokenized securities onchain — all while maintaining investor protection guardrails and continuing enforcement against bad actors.
- **Public market revitalization** — A "Make IPOs Great Again" push aimed at reversing the long-term decline in public companies. This includes proposed reforms to the disclosure regime intended to reduce compliance burdens and lower the barrier to going public, guided by a materiality standard, while still preserving core investor protections. Atkins frames this as expanding access: fewer IPOs means fewer everyday investors get the chance to participate in the growth of new American companies.
- **Private market access** — A proposal to expand retail investor participation in private markets, which Atkins argues have historically been reserved for wealthy institutional insiders, paired with appropriate safeguards to protect retail participants entering that space.

Atkins closed by tying the agenda to the SEC's broader statutory mission — protecting investors, facilitating capital formation, and maintaining fair, orderly, and efficient markets — and to a longer-term ambition of keeping U.S. capital markets the deepest and most dynamic in the world.

Sonia Agnesod

Planning, Coordination, and Compliance

Empowering a Mission-Driven Nonprofit with PCI DSS Assessment Support

USA for IOM demonstrated alignment with applicable PCI DSS requirements within the defined assessment scope and established a stronger foundation for managing compliance responsibilities independently. Key outcomes included:

1) Secure acceptance of digital donations as an independent nonprofit Increased donor confidence and readiness for future fundraising growth

2) Robust policies and documentation aligned to industry best practices

3) Clear understanding of renewal timelines and vendor expectations

4) Quarterly vulnerability scanning and long-term compliance planning

Most importantly, the organization emerged more confident, prepared, and informed as it continued to scale its digital fundraising capabilities.

"They Didn't Just Guide Us — They Partnered With Us.

Despite our limited technical knowledge, RSI made the process approachable by explaining requirements in plain language and helping us understand what was needed from our vendors and systems."

PARTNER HIGHLIGHT

RS Assurance & Advisory

For SaaS platforms, cloud providers, and any vendor entrusted with customer data, SOC 2 has moved from differentiator to requirement. Prospects ask for the report before they sign. RSI Security helps organizations get there — and stay there — with SOC 2 readiness and attestation support delivered alongside our partner, RSAA.

Why SOC 2 Matters:

SOC 2 is a demonstration that your controls for security, availability, and confidentiality are not just designed on paper but operating effectively over time. For growing companies, it is often the gate to enterprise deals, and increasingly a baseline expectation in vendor risk reviews. The challenge is rarely intent — it is scoping the environment correctly, collecting defensible evidence, and sustaining controls between reports.

How RSI Security Helps:

RSI Security brings the readiness discipline that determines whether a SOC 2 engagement is smooth or painful. We help define scope, map your controls to the Trust Services Criteria, identify and close gaps before they become findings, and organize evidence so the attestation process moves efficiently. This is the same "prepare properly, assess once" approach that runs through everything we do — the assessment goes better when the groundwork is solid.

Delivered With RSAA:

SOC 2 services are delivered in partnership with RSAA, extending RSI Security's ability to support organizations through readiness and attestation. The combination pairs RSI Security's cross-framework compliance expertise with RSAA's SOC 2 delivery — so clients get a coordinated path rather than a handoff between disconnected vendors.

At a Glance: RSAA

They prepare organizations for compliance audits. We do not conduct attestations for clients we've advised. That's not a limitation, it's the entire structure that makes our work valuable to you and credible to the people reading your report. If you're evaluating compliance advisors and want to understand exactly what the right engagement looks like, we're happy to walk through it.

Frameworks: CMMC · NIST 800-171 · NIST 800-53 · HIPAA · ISO 27001 · SOC 2 · PCI DSS

"By pausing [CMMC] Phase 2 implementation, we are keeping more companies in the DIB who would otherwise be forced out of the market at a time when we need them most."

Michael Duffy, DoD Official

UPCOMING TRANSITIONS

What Is Changing Across Our Services

FedRAMP Readiness

FedRAMP Launches Consolidated Rules for 2026.

FedRAMP announced its Consolidated Rules for 2026 on June 25, formalizing FedRAMP 20x as a widely available certification path (no longer just a pilot) alongside the legacy Rev5 process, which is now on a defined sunset timeline. Key dates: FedRAMP Ready submissions close July 28, 2026; Rev5 certification submissions stop being accepted entirely by June 11, 2027; and all current Rev5-certified systems must adopt the new Consolidated Rules by January 1, 2027. For cloud service providers on the FedRAMP path, the message is clear — start reviewing the new rules now, since both the 20x pipeline (opening in phases starting August 3) and the Rev5 transition timeline are moving fast.

HITRUST Assessment

HITRUST Key Updates. HITRUST closed the comment period on July 1 for proposed updates to select HITRUST CSF certification requirements. The changes target risks from frontier AI models, aligning with the "Defend" and "Thwart" areas of the NIST Cyber AI Profile — covering vulnerability, configuration, and incident management controls.

On the platform side, HITRUST is rolling out a Report Center Dashboard update targeted for Q3 2026: completion letters in MyCSF will include direct links and QR codes to assessment dashboards, giving organizations more direct control over how they share reports with relying parties. HITRUST confirmed this is a delivery/access change only — core testing, scoring, and QA rules for certification remain unchanged.

GDPR Advisory

GDPR Landscape. The European Data Protection Board (EDPB) issued several notable updates this month. It published draft Guidelines on Anonymisation, adopting a "relative" approach to identifiability — open for public consultation through October 30, 2026. The EDPB also finalized its guidelines on blockchain processing, confirming that hashed or encrypted on-chain data still qualifies as personal data and does not override an individual's right to erasure — a significant clarification for any blockchain-based data architecture. Separately, the EDPB launched a public consultation (closing August 5, 2026) on a standardized digital incident notification template for breach reporting.

The Secure Brief

Partnership Beyond the Assessment

RESOURCES

New For Your Organization

1. **Preparing for FedRAMP?** Check out our new readiness checklist to get your organization ready from an outside 3PAO assessor.
2. **Cyber Maturity Scorecard.** See where your program stands across people, process, and technology in roughly five minutes.
3. **Unified Federal Compliance Roadmap.** A plain-language guide to navigating CMMC and FedRAMP together, built around the November Phase 2 runway.
4. **AI Governance Readiness Guide.** Build a defensible program across ISO 42001, NIST AI RMF, and HIPAA before AI tools become mandatory inventory line items.
5. **Weekly Threat Report.** The short-form companion to this monthly brief, tracking the threats that matter as they break.

Where to Start

If one theme runs through this issue, it is that the fundamentals still decide outcomes. An accurate asset inventory, disciplined patch prioritization, third-party and OAuth visibility, and compliance built to sustain rather than expire are not advanced moves. They are the baseline, and they are still where most breaches begin.

RSI Security helps regulated organizations turn that baseline into a defensible, continuous program, from CMMC and FedRAMP readiness to AI governance and continuous cyber maturity, with advisory continuity that does not end when the assessment does.

YOU HAVE QUESTIONS

Our Team Has Answers

info@rsisecurity.com
Southlake, TX
rsisecurity.com
(858) 252-2448